AMENDMENTS TO THE CLAIMS

CLAIMS (clean copy)

1. (currently amended) A method for transmitting digital data in a form of packets through a transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit, the method comprising the steps of:

(a) encoding a sent data packet to form a sent encoded data packet having an "M" eight-bit bytes Protected Packet and an "n" D-parity field ;

(b) transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the sent encoded data packet being received as a received encoded data packet at the output of the transmission medium, the received encoded data packet having an "M" eight-bit bytes Protected Packet and an "n" D-parity filed, the Protected Packet comprising the sent data packet of the sent encoded data packet and a data packet of the received encoded data packet;

(c) checking for errors in the data of the Protected Packet of the received encoded data packet, and if an error occurred, applying an error correction scheme for computing an error correction field for said error and inserting said error correction field in the "n" D-parity field;

(d) computing, for said error correction field, an error Syndrome field having "k" error syndrome subfields, and if numbers of bits in the "k" error syndrome subfields are equal, applying the error correction field to correct the error of the sent data packet, otherwise, dropping the sent data packet; and

(e) decoding the received encoded data packet to recover a copy of the sent data packet.

2. (currently amended) A method as described in claim 1, wherein the step (a) comprises encoding the sent data packet to form the sent encoded data packet having the "M" eight-bit bytes Protected Packet, wherein the Protected Packet has data fields

having "x" bytes of data, and a cyclic redundancy code (CRC) field having "y" bytes such that " x + y" equals to "M".

2a. (new) A method as described in claim 2, wherein the CRC field comprises a detection field of the sent encoded data packet and a detection field of the received encoded data packet.

2b. (new) A method as described in claim 2, wherein "M"= 66, "x"= 64, and "y"=2.

3. (currently amended) A method as described in claim 1, wherein the step (c) further comprises calculating data parity in the "n" D-parity field, and wherein "n" equals to three (3).

3a. (new) A method as described in claim 3, wherein the "n" D-parity field comprises a correction field of the sent encoded data packet and a correction field of the received encoded data packet.

4. (original) A method as described in claim 2, wherein the step of correcting errors comprises correcting one or more errors occurred in a single data word of the Sent Encoded Packet only.

5. (currently amended) A method as described in claim 1, wherein the step (d) comprises generating a packet drop indicator signal if the power of the correction scheme is exceeded and the correction scheme cannot correct errors.

6. (currently amended) A method as described in claim 5, wherein the step (d) comprises generating a packet drop indicator signal if the integrity of the data of said Protected Packet is not confirmed.

7. (currently amended) A method as described in claim 1, wherein the step (d) comprises applying an algebraic function to the data words in the data of said Protected Packet to generate respective error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet.

8. (currently amended) A method as described in claim 1, wherein the step (d) comprises:

(k) applying an algebraic function to the data words in the data of said Protected Packet to generate respective error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet;

(l) applying a bitwise exclusive OR function to said generated error correction fields to obtain corresponding error syndrome values, and if an error occurred, identifying the data word which has the error and obtaining a bit pattern of the error from the error syndrome values; and

(m) correcting the identified word in the data of said Protected Packet by using the obtained bit pattern to obtain a corrected Protected Packet.

9. (original) A method as described in claim 7, wherein the step of applying the algebraic function comprises performing a N-dimensional parity calculation.

10. (original) A method as described in claim 9, wherein the step of applying N-dimensional parity calculation comprises performing a 3D (three dimensional) parity calculation.

11. (currently amended) A method as described in claim 1, wherein the step (c) comprises applying an algebraic function to the data words in the sent data packet of the Protected Packet to generate a detection field.

12. (original) A method as described in claim 11, wherein the step of applying the algebraic function comprises applying one or more of the following functions: CRC-16, CRC-32 and a checksum.

13. (currently amended) A method as described in claim 7, wherein the step of determining the integrity of the data of said Protected Packet comprises:

(n) applying said error detection scheme to the data of the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet of said Protected Packet to generate respective detection fields;

(p) comparing the generated detection fields; and

(q) confirming the integrity of the data of the Protected Packet, if the generated detection fields are equal.

14. (original) A method as described in claim 10, wherein the transmitting of data is performed so that each data word is an 8-bit byte, and each data packet has not more than 64 bytes.

15. (original) A method as described in claim 1, wherein transmitting of the sent encoded data packet through the transmission medium comprises transmitting said packet through the transmission link.

16. (original) A method as described in claim 15, wherein transmitting the sent encoded data packet through the transmission link comprises transmitting said packet through the link which provides line coding of the transmitted data.

17. (original) A method as described in claim 16, wherein the transmitting the packet through the line coded link comprises transmitting the packet through the link, which provides 8B/10B line coding.

18. (currently amended) A system for transmitting digital data in a form of packets through a transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit, the system comprising:

(1) an encoder, encoding a sent data packet to form a sent encoded data packet having an "M" eight-bit bytes Protected Packet and an "n" D-parity field;

(2) a transmitter, transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the sent encoded data packet being received as a received encoded data packet at the output of the transmission medium, the received encoded

data packet having an "M" eight-bit bytes Protected Packet and an "n" D-parity filed, the Protected Packet comprising the sent data packet of the sent encoded data packet and a data packet of the received encoded data packet;

(3) a detector, checking for errors in the data of the Protected Packet of the received encoded data packet, and if an error occurred, applying an error correction scheme for computing an error correction field for said error and inserting said error correction field in the "n" D-parity field;

(4) a corrector, computing, for said error correction field, an error Syndrome field having "k" error syndrome subfields, and if numbers of bits in the "k" error syndrome subfields are equal, applying the error correction field to correct the error of the sent data packet, otherwise, dropping the sent data packet; and (5) a decoder, decoding the received encoded data packet to recover a copy of the sent data packet.

19. (currently amended) A system as described in claim 18, wherein the corrector comprises means for correcting errors in the data of the Protected Packet of the received encoded data packet.

19a. (new) A system as described in claim 18, wherein the detector comprises means for calculating data parity in the "n" D-parity field, and wherein "n" equals to three (3).

20. (currently amended) A system as described in claim 19, wherein the corrector further comprises means for storing the "M" eight-bit bytes Protected Packet in a two-dimensional array of bytes.

20a. (new) A system as described in claim 20, wherein the corrector has a random access memory for storing the two-dimensional array of bytes of the "M" eight-bit bytes Protected Packet.

21. (original) A system as described in claim 19, wherein the means for correcting errors comprises means for correcting one or more errors occurred in a single data word of the Sent Encoded Packet only.

22. (currently amended) A system as described in claim 18, wherein the corrector comprises means for generating a packet drop indicator signal if the power of the correction scheme is exceeded and the correction scheme cannot correct errors.

23. (currently amended) A system as described in claim 22, wherein the corrector further comprises means for generating a packet drop indicator signal if the integrity of the data of said Protected Packet is not confirmed.

24. (currently amended) A system as described in claim 22, wherein the corrector comprises means for applying an algebraic function to the data words in the data of said Protected Packet to generate respective error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet.

25. (currently amended) A system as described in claim 18, wherein the corrector comprises:

(w) means for applying an algebraic function to the data words in the data of said Protected Packet to generate error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet, respectively;

(x) means for applying bitwise exclusive OR function to said generated error correction fields to obtain corresponding error syndrome values;

(y) means for identifying the data word which has the error, if any, and means for obtaining a bit pattern of the error from the error syndrome values; and

(z) means for correcting the identified word in the data of said Protected Packet by using the obtained bit pattern to obtain a corrected Protected Packet.

26. (original) A system as described in claim 24, wherein the means for applying the algebraic function comprises means for performing a N-dimensional parity calculation.

27. (original) A system as described in claim 26, wherein the means for

performing the N-dimensional parity calculation comprises means for performing a 3D (three dimensional) parity calculation.

28. (currently amended) A system as described in claim 18, wherein the detector comprises means for applying an algebraic function to the data words in the sent data packet of the Protected Packet to generate a detection field.

29. (original) A system as described in claim 28, wherein the means for applying the algebraic function comprises means for applying one or more of the following functions: CRC-16, CRC-32 and a checksum.

30. (currently amended) A system as described in claim 25, wherein the means for determining the integrity of the data of said Protected Packet comprises:

(i) means for applying said error detection scheme to said data of the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet of said Protected Packet to generate respective detection fields;

(ii) means for comparing the generated detection fields;and

(iii) means for confirming the integrity of the data of the Protected Packet, if the generated detection fields are equal.

31. (original) A system as described in claim 27, wherein each data word is an 8-bit byte, and each data packet has not more than 64 bytes.

32. (original) A system as described in claim 18, wherein the transmission medium comprises a transmission link.

33. (original) A system as described in claim 32, wherein the transmission link comprises a line encoder for transforming each "p" bits of said sent encoded data packets into "q" bits, "q" being not less than "p", and a line decoder for transforming each of the received "q" bits into "p" bits of said received encoded data packets.

34. (original) A system as described in claim 33, wherein "p"=8 and "q"=10.

35. (currently amended) An encoder for the system described in claim 18 for transmitting digital data in a form of packets through a transmission medium with error correction, comprising:

(6) a detector, adding an error detection field to the Protected Packet of the sent encoded data packet;

(7) a corrector, adding a respective error correction field to the Protected Packet of the sent encoded data packet; and

(8) a transmitter, sending the sent encoded data packet to the transmission medium.

36. (original) An encoder as described in claim 35, wherein the means for adding the error detection field comprises means for adding the error detection filed according to one the schemes: CRC-16, CRC-32 and checksum.

37. (original) An encoder as described in claim 35, wherein the means for adding the error correction field comprises means for applying 3D parity calculation to the Protected Packet.

38. (currently amended) A decoder for the system described in claim 18 for receiving digital data in a form of packets from the transmission medium with error correction, the decoder comprising:

(iv) a receiver, receiving the received encoded data packet from the transmission medium; and

(v) a corrector, correcting errors, if any, in the received encoded data packet to recover a corrected Protected Packet which includes fields from the Protected Packet with the errors being corrected; and (vi) a detector, determining integrity of the data of the corrected Protected Packet; and recovering a corrected data packet from the corrected data of the Protected Packet, the corrected data packet being a copy of the sent data packet.